Section II: **Administrative Security**
Title: **Information Security and Compliance Management Issues Standard**
Current Effective Date: **June 30, 2008**
Revision History: **June 18, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To ensure that the North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices comply with federal and state laws and regulatory compliance security requirements.

STANDARD

1.0 Background

The Divisions and Offices management shall ensure that workforce members are in compliance with all federal, state and Department legal and regulatory requirements, standards, policies, procedures, and guidelines as required.

2.0 Complying with Legal and Regulatory Obligations

The Divisions and Offices management, with assistance from the Division Information Security Official (ISO), shall ensure that all workforce members are provided a summary of the legal and regulatory security compliance requirements (i.e., federal and state laws) that address the use of information technology systems and the protected data and/or information that reside on those systems. For the legal and regulatory security compliance requirements, refer to the NC Statewide Information Security Manual – Chapter 12, Section 01: Complying with Legal Obligations – Standard 120101: Being Aware of Legal Obligations.

3.0 Complying with Intellectual Property Laws

Where applicable, Divisions and Offices management shall provide appropriate workforce members with guidelines for obeying intellectual property right agreements related to associated technologies.

3.1 Using Copyrighted Information from the Internet, Reports, Books, and Documents

The Divisions and Offices must comply with all use copyright restrictions when disseminating information from reports, books, documents, or in any electronic format.

3.2 Complying with Database Copyright Laws

Divisions and Offices management shall inform their workforce members of any proprietary rights in databases (or similar compilations) and the appropriate use of such confidential data and/or information stored in databases.

3.3 Complying with Copyright and Software Licensing Requirements

Divisions and Offices management and Division ISOs shall establish policies, procedures, and guidelines for software usage, distribution, and removal. In order to ensure that the Divisions and Offices software usage meets and/or exceeds federal and state copyright and licensing regulations, the Division and Office policies, procedures, and guidelines shall include the development of internal controls to monitor the number of licenses available and the number of copies in use. These policies, procedures, standards, and guidelines shall be monitored routinely and included in the Business Continuity Plan (BCP), Continuity of Operations Plan (COOP), and Disaster Recovery Plan (DR) in order to meet security compliance.

DHHS workforce members involved in the illegal reproduction of software can be subject to civil damages and criminal penalties. DHHS workforce members shall obey licensing agreements and shall not create, acquire, or use unauthorized copies of commercial software on Division and Office technology devices.

4.0 Legal Safeguards Against Computer Misuse

When using information resources, Divisions and Offices management must ensure that workforce members abide by the Acceptable Use for DHHS Information Resources policy. Management must also provide workforce members with any other applicable legal policy requirements.

5.0 Managing Media Storage and Record Retention

For records created or received in the course of performing state business, the Divisions and Offices are required to formulate complete and accurate record retention and disposition schedules that comply with the provisions of the NC General Statutes (N.C.G.S.) § 121-5 Public Records and Archives and the N.C.G.S. § 132-1 *et seq.* "Public Records". Divisions and Offices management must manage their records according to the schedules, as approved by the NC Department of Cultural Resources (DCR) – Government Records Branch of NC, throughout the record's life cycle from creation to disposition.

6.0 Complying with Information Security Standards and Policies

Divisions and Offices shall comply with applicable federal, state, and Department legal and regulatory requirements, standards, policies, procedures, and guidelines. Refer to the NC DHHS Security Standards, Administrative Security Standards – Information Security Training and Awareness Standard for additional information.

7.0 Other Compliance Issues - Recording Evidence of Information Security Incidents

Refer to the NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual, Information Incident Management Policy.

Reference:

- HIPAA Administration Simplification Act - 45 C.F.R. Parts 160 and 164.
  - HIPAA – 45 C.F.R. § 160.500 Applicability.
  - HIPAA – 45 C.F.R. § 164.105 (a)(2)(ii)(C) Safeguard Requirements.
  - HIPAA – 45 C.F.R. § 164.308 Administrative Safeguards.
  - HIPAA – 45 C.F.R. § 164.308 (a)(1) Security Management Process.
  - HIPAA – 45 C.F.R. § 164.308 (a)(5)(ii)(B) Protection from Malicious Software.
  - HIPAA – 45 C.F.R. § 164.308 (a)(6)(i) Security Incident Procedures.
  - HIPAA – 45 C.F.R. § 164.308 (a)(7)(i) Contingency Plan.
  - HIPAA – 45 C.F.R. § 164.312 (b) Audit Controls.
  - HIPAA – 45 C.F.R. § 164.312 (c)(2) Integrity and (e)(2)(i) Integrity Controls.
  - HIPAA – 45 C.F.R. § 164.318 Compliance Dates for the Initial Implementation of the Security Standard.
  - HIPAA – 45 C.F.R. § 164.502 (a)(b)(c)(d)(e)(f)(g)(h)(i)(j) Uses and Disclosures of Protected Health Information: General Rules.
  - HIPAA – 45 C.F.R. § 164.504 (a)(b)(c)(e)(g) Uses and Disclosure: Organizational Requirements.
  - HIPAA – 45 C.F.R. § 164.512 (e)(f) Legal Occurrences.
    - HIPAA – 45 C.F.R. § 164.512 (e) Disclosure for Judicial and Administrative Proceedings.
    - HIPAA – 45 C.F.R. § 164.512 (f) Disclosure for Law Enforcement Purposes.
  - HIPAA – 45 C.F.R. § 164.520 (c) Implementation Specification: Provisions of Notice.
  - HIPAA – 45 C.F.R. § 164.530 (a)(b)(c)(d)(e)(f)(g)(h)(i)(j)(k)(l) Administrative Requirements.
  - HIPAA – 45 C.F.R. § 164.534 (a)(b)(1) Health Plans Other Than Small Health Plans.

- North Carolina General Statutes
  - N.C.G.S. § 121-5. Public Records and Archives.
  - N.C.G.S. § 132-1. *et seq.* "Public Records" defined.
  - N.C.G.S. § 147-33.111. State CIO Approval of Security Standards and Security Assessment.

- NC Department of Cultural Resources (DCR)
  - Government Records Branch of NC

- NC Statewide Information Technology Security Manual, Version No. 1
  - Chapter 12 – Complying with Legal and Policy Requirements, Sections 01: Complying with Legal Obligations
    - Standard 120101 – Being Aware of Legal Obligations
    - Standard 120102 – Complying with State and Federal Records Laws
    - Standard 120103 – Complying with General Copyright Laws
    - Standard 120104 – Complying with Database Copyright Law
    - Standard 120105 – Complying with Copyright and Software Licensing Requirements

- Standard 120106 – Legal Safeguards Against computer Misuse
  - Chapter 12 – Complying with Legal and Policy Requirements, Section 02: Complying with Policies
    - Standard 120201 – Managing Media Storage and Record Retention
    - Standard 120202 – Complying with Information Security Standards and Policy
  - Chapter 12 – Complying with Legal and Policy Requirements, Section 03: Avoiding Litigation
    - Standard 120302 – Using Copyrighted Information from the Internet
    - Standard 120303 – Sending Copyrighted Information Electronically
    - Standard 120304 – Using text Directly from Reports, Books, or Documents
    - Standard 120305 – Infringement of Copyright
  - Chapter 12 – Complying with Legal and Policy Requirements, Section 04: Other Legal Issues
    - Standard 120401 – Recording Evidence of Information Security Incidents
    - Standard 120404 – Recording Telephone Conversations
    - Standard 120407 – Reviewing System Compliance Issues

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Security Training and Awareness Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Information Incident Management Policy